

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MONTANA
HELENA DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

vs.

DERRICK LEE DRIVDAHL,

Defendant.

CR 13-18-H-DLC

Defendant Derrick Lee Drivdahl is charged with receipt and distribution of child pornography pursuant to 18 U.S.C. § 2252(a)(2). Drivdahl filed a motion to suppress all evidence acquired by the Helena Police Department as a result of the search warrant and supporting affidavit served at Drivdahl's residence on or about July 15, 2013, as well as evidence collected during Drivdahl's arrest on the same day, including statements made by Drivdahl, and the content of a thumb drive and Chromebook Laptop seized during the arrest. Drivdahl argues that his arrest was the result of a warrant to search his residence that was not supported by sufficient probable cause because it contained information collected as a result of previous illegal and unwarranted searches and/or improperly disclosed electronic

communications.

I. Factual Background

When Google discovers child pornography on its system, 18 U.S.C. § 2258A requires it to report its findings to the CyberTipline of the National Center for Missing and Exploited Children (“NCMEC”). Google’s precise protocol related to CyberTip reports is at the center of the instant motion, and will be discussed below.

The first CyberTip report related to this case was generated by Google and sent to the NCMEC in February of 2013. The NCMEC determined that the report should be sent to Pennsylvania for further investigation based on the IP address that Google provided. Ultimately, the Pennsylvania detective working the case determined through additional information obtained from Google via a warrant that the Gmail account (rdrivdahl@gmail.com) related to the report actually resolved to an IP address in Montana. The Pennsylvania detective sent his files on this tip to the Helena Police Department, where they ultimately landed on Detective Bryan Fischer’s desk on July 19, 2013.

Fischer filed a warrant application and affidavit in support thereof on July 15, 2013, based on this initial CyberTip, as well as subsequent CyberTips that he believed implicated Defendant Drivdahl of trafficking in child pornography in

violation of federal law. Several of these subsequent CyberTips were the result of an investigation conducted by Google employee Sean Zadig, who produced a supplemental report pertaining to Drivdahl's use of Google services to upload child pornography. Fischer used this supplement in conducting his own investigation, and referred to it and its contents in the affidavit. Fischer and Zadig were also in contact with each other following the submission of Zadig's supplement.

The resolution of this motion hinges on the nature and chronology of the relationships between Mr. Zadig, Google as the supplier of CyberTips related to Mr. Drivdahl, and Detective Fischer. The crux of Mr. Drivdahl's argument is that Google and/or Mr. Zadig were government actors for purposes of the Fourth Amendment, and that as such, a warrant was required prior to their obtaining and viewing the materials upon which Fischer's affidavit was based.

II. Legal Standard

The Fourth Amendment assures that "the right of the people to be secure in their persons, houses, papers and effect, against unreasonable searches and seizures, shall not be violated." U.S. Const. Amend. IV. Because the Fourth Amendment constrains government searches and seizures, it does not apply "to a search or seizure, even an unreasonable one, effected by a private individual not

acting as an agent of the Government or with the participation or knowledge of any government official.” *United States v. Jacobsen*, 466 U.S. 109, 113 (1984).

However, “[w]here a private party acts as an instrument or agent of the state in effecting a search or seizure, Fourth Amendment interests are implicated.”

Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971). The Ninth Circuit has established that when “determining whether a private party’s search implicates the Fourth Amendment, the relevant inquiry is (1) whether the government knew and acquiesced in the intrusive conduct; and (2) whether the party performing the search intended to assist law enforcement efforts or further his own ends.” *United States v. Cleveland*, 38 F.3d 1092, 1093 (9th Cir. 1994) (internal quotations and citations omitted). “The government must be involved either directly as a participant or indirectly as an encourager of the private citizen’s actions before we deem the citizen to be an instrument of the state. The requisite degree of governmental participation involves some degree of knowledge and acquiescence in the search. *United States v. Walther*, 652 F.2d 788, 791-92 (9th Cir. 1981) (internal quotations and citations omitted); *see also United States v. Sherwin*, 539 F.2d 1, 6 (9th Cir. 1976) (holding that “a private person cannot act unilaterally as an agent or instrument of the state; there must be some degree of governmental knowledge and acquiescence. In the absence of such official involvement, a search

is not governmental.”). Finally, the defendant bears the burden of “establishing government involvement in a private search.” *Id.*

Of course, the results of an illegal search cannot be included in a warrant affidavit to establish probable cause. *See, e.g., United States v. Vasey*, 834 F.2d 782 (9th Cir. 1987).

III. Discussion

The Court notes at the outset that much of Drivdahl’s brief supporting his motion to suppress is admittedly based on assumptions of fact regarding Google’s internal procedures and the relationship between Google and Detective Fischer. As will be discussed at length below, the government’s response brief and the supporting affidavit of Sean Zadig clarify many of the ambiguities and dispel many of the assumptions contained in Drivdahl’s initial brief. The Court will first address the arguments raised in this initial brief, and will then turn to the arguments Drivdahl advanced after receiving the government’s response and Zadig’s affidavit.

Drivdahl essentially advances two “joint endeavor” arguments in which he claims Google was in fact operating as a government agent for the purposes of Fourth Amendment protection, each of which will be discussed in turn.

A. Sean Zadig and Google Were Not Government Actors

Drivdahl's primary argument is based on its understanding that after Google provided NCMEC several CyberTips, it became an "agent of the government, through employee Sean Zadig, by analyzing data, disclosing other electronic communications beside child pornography and generally aiding law enforcement (*i.e.* Detective Fischer) to determine the connections and interrelationships between and among various email addresses and accounts that were for the most part all connected to defendant's residence." (Doc. 18 at 11.) Defendant claims that this was a joint endeavor subject to Fourth Amendment protection because "Google, the NCMEC and Detective Fischer teamed up to review and analyze any and all of the electronic data connected to defendant's email address(es) for the express purpose of preparing the search warrant application for defendant's residence." (*Id.*) Zadig's affidavit both sheds light on his and Google's exact roles in this investigation, and deflates Drivdahl's argument that either he or Google was acting as a government agent.

In addition to information contained in the initial CyberTips generated by Google pertaining to Drivdahl between February 2 and June 19, 2013, the search warrant affidavit also included information and analysis compiled by Sean Zadig in a supplemental report. Zadig testifies that on June 20, 2013, he conducted a

regular review of CyberTips that had been sent to NCMEC the previous day. Zadig discovered that one of the tips pertained to user “ilovlitrgrls@gmail.com,” who had additional accounts that contained sexual images, and who had made posts and comments within his Google+ Circles and Communities that appeared to solicit materials related to child sexual abuse from other users, and describe his employment with his school and his access to children. (Doc. 25 at 2.) Based on this information, Zadig launched an extensive investigation during which he identified accounts that shared attributes with the “ilovlitrgrls@gmail.com” account, and reviewed the subscriber information, images stored in the Google+ Photos service, and posts made through the Google+ service associated with those accounts. (*Id.*) Zadig clarified that he did not have access to nor review any Google messages (emails). Following his investigation, Zadig emailed his results to NCMEC on June 24, 2013 in the form of a supplemental report. Drivdahl contends that this supplement was constructed by Zadig as a government agent and is the product of “teaming up” between Zadig and Fischer. Critically, however, Zadig testified that at no time prior to the transmission of the report on July 24, 2013 did he speak to any government entity or officer regarding the subject matter of that report, and Drivdahl offers no evidence that calls this assertion into question.

Turning to the first prong of the *Cleveland* analysis, there is simply no evidence that Fischer or any government agent was aware of Zadig's investigation – let alone acquiesced or encouraged it – until it was completed and sent to Fischer via NCMEC. Here, the government was not involved directly or indirectly as a participant or encourager, nor did it have any degree of knowledge or acquiescence. *Walther*, 652 F.2d 791-92. There is simply nothing in the record to suggest that law enforcement agents were involved in the search or investigation of Drivdahl's activities until after Zadig reported his discoveries to NCMEC.

Both parties discuss the second prong of the *Cleveland* analysis, but since the question of government knowledge is dispositive, the Court need not delve into Zadig's motivation for compiling his report.

While the Court is presented with no evidence that Zadig's June 24, 2013 report to the NCMEC was a "joint endeavor," Zadig and Fischer did speak several times after that point. On June 25, 2013, NCMEC informed Zadig that it had sent his supplement to the Billings Police department. The following day Zadig contacted Fischer to ensure that the supplement had reached him, because he feared that there could be an imminent risk to minors, given that the subject of the CyberTip and his supplement was potentially an elementary school janitor. Zadig also states that he did communicate with Fischer while Fischer was conducting his

own investigation and preparing his search warrant affidavit. However, these conversations were limited to general questions about Google services and to Zadig explaining the information that had been reported in the CyberTips and his supplement. Finally, in July of 2013, Zadig and Fischer exchanged several emails regarding the status of the case, but Zadig testified unequivocally that after he filed his supplement, no “additional user data was requested or disclosed,” and that he did not take any “further investigative steps.” (Doc. 25 at 3.)

The Court has no evidence before it to contradict Mr. Zadig’s sworn testimony. It is clear that Mr. Zadig conducted his investigation as a private citizen without any law enforcement contact or involvement. Thus, there is no basis to suppress the information that Zadig and Google gathered and subsequently provided to the government. “[O]nce a private search is completed, the subsequent involvement of government agents does not retroactively transform the original intrusion into a governmental search. *United States v. Sherwin*, 539 F.2d 1, 6 (9th Cir. 1976).

B. The Government Did Not Expand Upon the Information Provided to it as the Result of Google’s Practice of Identifying, Investigating, and Reporting Child Pornography on its Systems

In a related but ancillary argument, Drivdahl assumes that Google did not actually open any of the files upon which it based its CyberTips, but merely sent

the tips along to the NCMEC. Thus, so the argument goes, a government agent – either Google or Fischer – opened Drivdahl’s electronic files without a warrant. The Court has already established that Google, acting through Zadig, was not a government actor. Therefore, the only question that remains is whether Fischer or the NCMEC opened Drivdahl’s previously unopened files, thus expanding upon the private searches conducted by Google. The uncontested testimony in Zadig’s affidavit dispenses with this argument as well.

Once again, the evidence used to support probable cause for the search warrant consisted of a number of CyberTips that Google prepared and sent to NCMEC from February to June of 2013, as well as Zadig’s supplement. Zadig’s affidavit sheds light on precisely how Google handles its CyberTip reporting. Zadig testified that Google has a strong business interest in ensuring that its products are free of materials depicting child sexual abuse, and that eradicating such materials is “critically important to protecting our users, our product, our brand, and our business interests.” (Doc. 25 at 1.) To serve this interest, Google has a structured and formalized approach to ferret out child pornography. Part of Google’s standard procedure involves a member of the Legal Removals Team opening “each reported image file to confirm that it appeared to meet the statutory definition of child pornography . . . prior to submitting a CyberTip report.” (Doc.

25 at 2.) Unlike in *United States v. Keith*, 2013 WL 5918524 (D. Mass. Nov. 5, 2013) where AOL’s internal process for discovering child pornography relied entirely on algorithmic “hash value” information, the suspect material was opened by a Google employee prior to being turned over to the government. Thus, there was no expansion of the private search, which would have required a warrant.

C. Electronic Communications Privacy Act

Drivdahl’s final point in his initial brief is that Google violated the Electronic Communications Privacy Act (“ECPA”), 18 U.S.C. § 2701, *et seq.* Drivdahl simply has not sufficiently alleged or provided support for his claims that Google violated the ECPA, and that Zadig’s supplement exceeded the bounds of what is permitted by 18 U.S.C. § 2258A. The government is correct that according to Zadig’s unchallenged testimony, he did not have access to and did not review any Gmail messages (emails) of Google Talk/Hangout messages. His investigation was limited to posts and comments that Zadig observed within Google+ Circles and Communities.

Finally, even if Drivdahl succeeded in establishing or even sufficiently alleging an ECPA violation, suppression is not a remedy for violations of the ECPA in this situation. *See United States v. Cray*, 450 F. App’x 923, 930 (11th

Cir. 2012) *cert. denied*, 133 S. Ct. 265, 184 L. Ed. 2d 45 (U.S. 2012) (“In interpreting the Wiretap Act, 18 U.S.C. §§ 2510–2522, which Title I of the ECPA amended to address the interception of electronic communications, we held that, ‘while the Wiretap Act clearly provides criminal and civil sanctions for the unlawful interception of electronic communications, the Act provides no basis for moving to suppress such communications.’ *United States v. Steiger*, 318 F.3d 1039, 1046 (11th Cir. 2003) (citation omitted). We stated that ‘[d]espite the fact that the ECPA amended numerous sections of the Wiretap Act to include ‘electronic communications,’ the ECPA did not amend § 2515,’ which authorized suppression of evidence as a remedy solely for the illegal interception of wire and oral communications, but not for electronic communications. *Id.* at 1050. We concluded that the Wiretap Act did not provide a statutory suppression remedy for unlawfully acquired electronic communications because ‘the legislative history makes clear that a statutory suppression remedy does not exist for unlawful interceptions of ‘electronic communications.’ *Id.* at 1051.”); *United States v. Perrine*, 518 F.3d 1196, 1202 (10th Cir. 2008) (“[S]ection 2708 of the ECPA specifically states that ‘[t]he remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.’ 18 U.S.C. § 2708. Section 2707, in turn, describes remedies for

violations of the Act as including civil actions for violators other than the United States and administrative discipline against federal employees in certain circumstances. 18 U.S.C. § 2707. Thus, violations of the ECPA do not warrant exclusion of evidence.”).

D. Additional Arguments Raised in Defendant’s Reply Brief

In light of Zadig’s testimony, Drivdahl advances several new arguments in his reply brief, none of which the Court finds compelling.

First, Drivdahl points to the fact that in his affidavit Fischer stated, “Your Affiant also received a detailed supplement from Zadig,” whereas the government states in its response brief that Zadig’s report was first sent to the NCMEC.

Drivdahl is trying to create doubt where there is none, and even if there was, it would not pertain to a relevant point. Zadig testified that he sent his supplement to NCMEC and then called Fischer to alert him to the supplement. Drivdahl presents no evidence supporting any differing or inconsistent course of events. Fischer’s statement in his affidavit is most naturally construed to mean that he received a supplement prepared by Zadig. Even if Fischer received the supplement directly from Zadig, a theory that is wholly unsupported, it does not change the dispositive fact established above that Zadig prepared that supplement independent of any government influence, knowledge, encouragement, or acquiescence.

Drivdahl next takes issue with the fact that the warrant affidavit does not state that Google personnel opened and examined the relevant files to conclude that they contained child pornography. While such information would have been helpful in constructing the whole story, this Court will not conclude that absent such information, a reasonable magistrate must assume that it was the police that first opened and viewed the images rather than Google. In fact, the precise language of the affidavit that Drivdahl sites would more likely lead a magistrate to the conclusion that Google viewed the images prior to submitting the CyberTip: “Google reported on June 6, 2013, a user uploaded images of what appeared to be children under the age of 18 engaged in sexually explicit conduct . . .” (Doc. 20 at 56 (emphasis added).) This language implies that the images were viewed by human eyes, and not merely sent off the NCMEC after being algorithmically tagged as a hash value match with known images of child pornography, as was the case in *Keith*.

Finally, Drivdahl states that Mr. Zadig’s supplement exceeded the scope of the reporting requirements established by § 2258A(b)(1)-(5), and that under §§ 2258A-2258E Google is authorized to run scans on electronic communications to detect hash values that evidence the existence of child porn, but is not permitted to open or view files to discover child porn (Doc. 26 at 7.) While § 2258A does not

explicitly authorize ISPs to open and view files suspected of containing child pornography, it certainly does not preclude an ISP from doing so, especially if it serves a business interest such as the one articulated by Zadig and recognized as valid by courts in the past. *See United States v. Cameron*, 699 F.3d 621, 638 (1st Cir. 2012); 18 U.S.C. § 2510(5)(a)(ii). The end result of the paradigm Drivdahl advances is that ISPs may not view any files suspected of containing images of child pornography, but must instead forward them blindly to the NCMEC, which must obtain a warrant to view the files, or forward them to law enforcement who must obtain a warrant. This constraint upon ISPs is not evident on the face of the statutes at issue, nor is it consistent with the case law that takes no issue with ISPs viewing suspected child pornography prior to submitting CyberTips. *See id.*; *United States v. Richardson*, 607 F.3d 357 (4th Cir. 2010). Finally, even if Zadig had exceeded the parameters of permitted reporting, the fact remains that suppression is not an appropriate remedy for such a violation since Zadig was not acting as a government agent.

IV. Conclusion

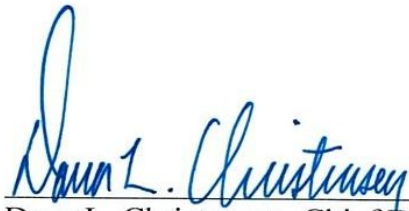
None of the evidence derived from the CyberTips reports generated by Google or from Zadig's supplement were gathered in contravention of the Fourth Amendment. There is sufficient evidence before the Court, including Detective

Fischer's affidavit in support of the warrant and Mr. Zadig's sworn testimony, such that a hearing on this motion is not required. Zadig and Google acted without government involvement, knowledge or encouragement. Mr. Drivdahl has not provided a basis upon which this Court may suppress any evidence in this case. Accordingly,

IT IS ORDERED that Defendant's motion (Doc. 17) is DENIED.

IT IS FURTHER ORDERED that the March 6, 2014 plea deadline is VACATED, and RESET for March 7, 2014. The remainder of the Court's February 13, 2014 order (Doc. 23) remains in full force and effect.

Dated this 6th day of March, 2014.



Dana L. Christensen, Chief District Judge
United States District Court